Social Media Safety Quiz

Quiz · Privacy Settings, Impersonation, Sextortion, And Stalker-Bait.

Social media is the largest privacy and impersonation risk most adults face. Test your knowledge across the platforms you use — and the threats specific to social.

Instructions

10 multiple-choice questions. Pick the BEST answer for each. Don't peek at the answer key on the next page. Score yourself at the end. There's no time limit, but most people finish in 5-7 minutes.

Questions

Q1. A 'celebrity' DMs you on Instagram saying they want to gift you cryptocurrency, but you need to send a small fee first. This is:

- **A.** A real opportunity from a fan-friendly celebrity
- **B.** An impersonation scam — celebrities don't DM strangers asking for money
- **C.** A legitimate giveaway
- **D.** Probably worth the small fee

Q2. Your Facebook account is set to public. Which of these is the smallest privacy risk?

- **A.** Your full name is visible
- **B.** Your profile photo is visible
- **C.** Your check-ins, vacation photos, and friends list are all visible
- **D.** You list your high school graduation year

Q3. What's the safest way to reset your password on a social platform?

- **A.** Click the 'Reset Password' link in any email claiming to be from the platform
- **B.** Open the platform's app or website directly and initiate the reset there
- **C.** Reply to the email with your current password
- **D.** Call the number in the email

Q4. You receive a Friend Request from someone claiming to be a friend you already have. This is most likely:

- **A.** Your friend forgot they had an account
- **B.** An impersonation account designed to scam your other friends
- **C.** A duplicate account from Facebook
- **D.** A normal account migration

Q5. An app on your phone wants to access your social media account 'for analytics.' You should:

- **A.** Grant access — apps need permissions
- **B.** Deny unless you specifically need that integration

C. Grant temporarily then revoke later

D. Grant only if the app is free

Q6. Which of these settings reduces tracking and data sharing the most?

A. Setting your account to private

B. Disabling 'Off-Facebook activity' (Meta)

C. Both A and B together

D. Wearing a different shirt

Q7. If a sensitive image of you (or a teen you care for) is being threatened with public release:

A. Pay the demand to make it stop

B. Don't pay — sextortion typically escalates after payment. Document, report to platform and police, save evidence

C. Ignore and hope it resolves

D. Delete all your accounts

Q8. What's a strong sign that a social media account has been hacked?

A. You see a new follower

B. Strange posts appear, friends report unusual messages from you, login alerts from unfamiliar locations

C. Your feed is showing different content than usual

D. The platform launched a new feature

Q9. Which of these gives a stalker the most useful information?

A. Your favourite movie

B. Photos with location metadata showing where you live, work, or your kids go to school

C. Your favourite colour

D. Your hobbies

Q10. When posting on social media, what's the safest practice for minors in your family?

A. Post their full names, schools, and photos publicly

B. Post only with consent (theirs and / or their parents'), strip metadata, set audience to friends/family only

C. Tag them in every post with their location

D. Make their accounts public to help them grow followers

Answer Key

Don't peek before completing the quiz. Read explanations even for answers you got right — they reinforce the why.

Q1: B — Celebrity-impersonation scams are rampant. Real celebrities don't DM strangers asking for money. The 'fee' is the scam.

Q2: D — Year of graduation alone is low risk. Aggregating name + photo + check-ins + friends list = stalker / fraud goldmine.

Q3: B — Always reset via the official app/site, never via links in emails. Phishing 'reset' emails are extremely common.

Q4: B — Account cloning. Impersonator copies the profile pic, sends friend requests to the real friend's network, then runs scams on the friends.

Q5: B — Grant only if you actively need the integration. 'Analytics' is often code for data mining. Default to deny.

Q6: C — Both layers help — private account limits visibility; off-Facebook activity disables cross-site tracking. Both maximise privacy.

Q7: B — Sextortion escalates after payment. Document everything, save evidence, report to platform AND law enforcement.

Q8: B — Look for behavioural anomalies — posts you didn't make, messages friends didn't get from you. Login alerts from new locations are early warnings.

Q9: B — Location metadata in photos reveals home, work, and routines. Strip metadata before posting. Disable auto-location-tagging in apps.

Q10: B — Minors deserve strict protection. Audience-limited, no metadata, family consent. Public minor accounts are a stalker / predator risk.

Scoring

Score	Level	What it means
0–4	Beginner	Your social media is a privacy / security risk. Run the Social Media Privacy Checklist today.
5–7	Intermediate	Decent awareness. Run the Browser Privacy Settings Tool and Privacy Settings Worksheet for a thorough
8–10	Advanced	Strong instincts. Help your family — especially teens and elderly — through this same quiz.